International Journal of Media & Cultural Politics
Volume 9 Number 3
 doi: 10.1386/macp.9.3.277_1

SANDRA BRAMAN
University of Wisconsin-Milwaukee

The geopolitical vs. the network political: Internet designers and governance

ABSTRACT

With the recognition that communication networks in general and the Internet in particular are not only infrastructural but socio-technical in nature comes the responsibility to think such networks through from the perspective of how they influence – and/or are – forms of power and governance. The notion of citizenship is one that appears relative to both social and technical systems, and thus at their conjuncture, because it is the concept through which the rights and responsibilities of individuals relative to governance are refracted. It was in fact the case that citizenship was a concern for those responsible for technical design of the Internet as that history both unfolded through and is recorded in the technical document series known as the Internet Requests for Comments, or RFCs. This paper analyzes the two types of citizenship of concern from the perspective of Internet design – geopolitical (oriented around the state) and network political (oriented around the network) – and interactions between the two as they were discussed within and affected the Internet design process. These network-inspired ideas about citizenship in turn contribute to the ongoing discussion about the evolution of new forms of citizenship in today's environment, including in particular those that are global and/or technological in nature.

KEYWORDS

citizenship
Internet history
socio-technical systems
infrastructure
RFCs
Internet protocols
theories of the state

The affordances offered by the Internet to the formation of global political communities have given life to conversations about global citizenship first raised, in various forms, in the nineteenth century. This notion itself is just one among the many types of conceptualizations of citizenship in play during contemporary transformations of law-state-society relationships. The concept of 'network citizenship' emerged among those who participated in the technical design of the Internet, involved in what we might refer to as the 'network political' environment as distinct from the 'geopolitical' as defined by the international system of United Nations-recognized states.

This article traces the evolution of the concepts, norms, and practices of network citizenship among those responsible for the design of what we now call the Internet by looking at the technical document series – the Internet Requests for Comments, or RFCs – that has been the medium for and record of the design process since its launch shortly after the ARPANet project began in 1969. Thinking in such political terms was an inevitable expansion of the engagement of these computer scientists and programmers with legal and policy issues in the course of discussions about technical design problems, their solutions and their translation into the technical standards (protocols) needed to make what we now call the Internet work.

The process of designing the network generated a strong sense of community (Braman 2011; Turner 2006) that rapidly grew in numbers after commercialization took place in 1993, making the network available to any one for any use (Abbate 1999; Mueller 2002). The network was intended to be international from its conception, and was so in terms of participation in the design process and intended uses incorporated into that process even before the 1972 addition of non-US nodes to the network. Within just a couple of years of the launch of the network design process (Braman 2012), the concept of network citizenship had become another way of conceptualizing global citizenship. Relationships between geopolitical and network political citizenship are, however, not yet resolved; as negotiations between the two types of processes unfold, they feed and interact with the evolution of the informational state (Braman 2007a). Now that we understand from Schudson (1998) that even when confined to informational terms, and even when talking only about one country, there are many different ways of thinking about what is meant by the notion of 'the good citizen,' articulations of good citizenship of either type within the RFCs are of keen interest.

THE EVOLUTION OF CITIZENSHIP

The idea, institutions and practices of citizenship have taken multiple forms, from the origins of the concept of the citizen in ancient Greece through the development of modern forms of citizenship in the Westphalian state, to the appearance of such a variety of ways of thinking about citizenship today that the foundational meanings of the concept are themselves being contested. Approaches that engage with citizenship as a global and/or technological matter receive particular attention here following a brief run through the major figures of the history of citizenship.

The very definition of the modern state involved establishing modern forms of citizenship that transformed royal subjects into active participants in governance (Turner 1992). Westphalian standards for citizenship provide a baseline and a highly recognizable model (Caporaso 2000), including an approach to territoriality that links geographic space, political space as

defined in terms of the reach of public authority (jurisdiction) and civic space as defined in terms of the domains within which individuals can expect to be able to exercise their rights and to which individuals have responsibilities. Within this space, governments have the right to rule, and citizens are those who can exercise rights and should fulfill responsibilities. Living within the state is not enough to make one a citizen, however. There can be denizens in a given geographic space who are subject to the law but do not have the full rights and responsibilities of citizens.

This is known as the Westphalian state because it was with the Westphalian agreements of 1648 that the relationships between those providing leadership within a given territory – and the resources and people of that territory – were clarified sufficiently to establish the foundation for a secular international system of states. Through these agreements, which concluded the 'Thirty Years War' that involved most of Europe in what is considered the longest continuous war in history in traditional terms, a working consensus was achieved on the structural units through which the exercise of power, flows of capital and communications have operated since that time. Once in place, over the next century or so, states developed their administrative structures and conceptualizations and expectations of citizens reified (Featherstone 1990).

T. H. Marshall's (1950) history of the evolution of citizenship rights provided a conceptual framework that both reflected and framed a great deal of thinking about citizenship during the twentieth century. Starting from the Westphalian assumptions regarding jurisdictional scope, Marshall distinguished three types of citizenship rights that evolved over time. *Civil rights* have origins in Roman law and provided the foundations of citizenship in the seventeenth century; they protect individuals' freedoms and their rights to participate actively in governance. *Political rights*, which developed over the course of the 18th century, provide procedural protections for political action, speech and the vote. *Social rights*, the product of the late nineteenth century, provide the support systems of the welfare state.

Various pressures can stimulate change in the forms, practices and expectations of citizenship. Held (1989) emphasizes that the legitimacy of any given configuration is affected by the extent to which a government is considered authoritative, fair and worthy of support. Leca (1992) makes a parallel argument regarding the effects of relative prosperity on a state's relationships with citizens. Globalization, changes in the nature of power, the formation of a significant regionally based transnational governance body (the European Union) and dissolution of another (the Soviet Union), and the many capacities for social relations of all kinds offered by the Internet brought about a great deal of discussion towards the close of the twentieth century about alternative ways of conceptualizing citizenship.

With legal globalization and other developments that have drawn allegiances away from the state, the concept of citizenship has itself fragmented. Forms of citizenship that include some but not all of the bundle of types of relationships between individuals and the state described by Marshall (1950) began to appear, often referred to as 'thin' citizenship (e.g., Caporaso 2000). Recent research has found that Europeans are torn between wanting 'thicker' citizenship at the local level and simultaneously preferring uniformity throughout the European Union, for example, although the two can be mutually exclusive (Henderson et al. 2013). For many, the sense of citizenship has become conditional due to both expansion (legitimization of additional identities) and contraction (one's citizenship identity plays out in private life,

even for those who live alone) (Elkins 1997). Current work on the nature of citizenship has shifted from a focus on the passive to the active in characteristics of interest, away from social rights and obligations and towards self-governance (e.g., Pathak 2013) and away from inclusiveness and towards social cohesion as the goal of policy (e.g., Eizaguirre et al. 2012).

There have been at least two rounds of theorization of citizenship in explicit relationship to technology. The first developed out of the push towards postnormal science that began in the 1980s in response to environmental concerns in Europe. This movement, now spread internationally under diverse names, urges democratization of decision-making about which big science projects in which to invest and about how to use the results of such research. This movement bases its claims on the argument that this is appropriate because the governmental resources that support large-scale capital-intense scientific research come from citizens and because the effects of uses of research findings fall on citizens as well. Frankenfeld (1992) introduced the notion of technological citizenship to refer to the role of individuals within a postnormal science system, Stevenson (2006) argued that global activities of technological citizenship is the only way to resist destructive developments, and a number of other researchers have also used the concept in a similar manner (e.g., Bovens 2002; Elam and Bertilsson 2003; Strijbos 2001). Valkenburg (2012) extracted three characteristics of technological citizenship from this literature, including what he calls the subject requirement (all citizens have access to decision-making about technologies), the object requirement (decision-making procedures are such that citizens can be involved in decision-making about all types of technologies) and the epistemological requirement (decision-making procedures must balance citizen input with the need for expertise).

The second round of theorization of citizenship oriented around technologies appeared at the conjunction of concerns about citizenship and about free speech on the Internet among those concerned about the quality of the public sphere and their ability to meaningfully participate in it. As Hermes put it, citizenship – 'that which binds us' (2006: 28) – is the key quality of interest when we talk about the public sphere. From this perspective, citizenship is a political identity made possible through the medium of the *res publica*, the public conversation through which we engage on matters of shared concern. Competing interpretations and practices provide affordances for different types of conversations and forms of agency (Mouffe 1992). This has significant implications for the design and architecture of the digital environment through which so much of what we do as citizens takes place in the twenty-first century. Its importance is increasingly recognized not only in the 'values in design' movement for information technologies but also by thinkers such as Felt and Fochler (2010) on 'machineries for making publics' and by researchers at 'governance labs' in places as diverse as the United States and Brazil who are working on the software and media needed to technologically support universal engagement in the public sphere. Relationships between regulating and being regulated are complex; citizen participation can also involve technologies that regulate those citizens themselves (Flear and Pickersgill 2013).

Sociological foundations for thinking about the institutional dimensions of citizenship can be found in Durkheim and other early sociologists who emphasized the roles of citizenship in divisions of labor and their complex interdependencies (Yeatman 1994). This dimension became dominant in the 'corporate citizenship' programs of companies such as IBM (Mattelart 1987),

development of the 'industrial citizen' via collective bargaining arrangements and the creation of 'internal states' within organizations (Davis, Kahn and Zaid 1990). The 'legalization' of corporations involves claims of jurisdictional authority as private governments, with the same ability to require responsibilities and offer protections that is available to geopolitically recognized 'public' governments in relationship to their citizens. Citizenship, then, is needed in order to have democracy once a governance structure is in place with enough substance that an organization can be influenced and when individuals are directly affected. There is a conundrum, however, that organizational responses to demands for citizenship-like rights can yield additional unforeseen, perhaps unforeseeable, mechanisms of control for the organization itself (Dandeker 1990).

Citizenship itself may be transnational (Kaarsholm 2013), and even very local ancient national battles have become global matters as a result of the war on terror, as happened in Bosnia (Erjavec 2009). Globalization has produced 'interpenetrated' jurisdictions, social processes and public spheres that no longer map onto each other, making it difficult to determine just where effective political activity can take place (Braman 1996). For citizens, national-level political action may not be sufficient when it comes to engaging actual loci of decision-making that may be international or global, take place at another level of the domestic social structure and/or be driven by decision-making of another political entity of like kind but other (Braithwaite and Drahos 2000; Randeira 2007). The same dilemma presents itself at the local level (Braman 2007b).

The notion of global citizenship has become accepted to such an extent that it can be found on undergraduate liberal arts curricula and, by the early twenty-first century, had at least been considered for law school curricula (Nussbaum 2003). There are now instances in which groups of individuals identify themselves as citizens of particular states even though those states do not in turn recognize them as such. Researchers analyzing developments of these kinds focus on acts of citizenship as their units of analysis, rather than individual citizens (e.g., Barbero 2012). Koenig-Archibugi (2012) has quite originally proposed a form of 'fuzzy' citizenship in which a state's responsibilities to any given citizen would depend on the nature of the expected impact on the individual and the likelihood that that impact would occur. Effectively, then, people now often have multiple citizenships, at different levels of the social structure, from the local to the international (Charnovitz 2003).

All of this is of more than metaphoric importance during a period in which many formerly public functions are themselves becoming privatized, co-regulation is increasing in importance as an approach to governance (e.g., Marsden 2011), and policy networks comprising both public and private sector actors are often the preferred – the more valid – unit of analysis (Marsh 1998). The development of citizenship as an identity and set of practices within the public sphere, its fragmentation in public and reconstitution in private environments and its multiplication and globalization across interpenetrated complex systems have been triggered by – and remain reliant upon – the capacities provided by information and communication technologies (Lee 2009). In the same way that the French phrase '*filiere electronique*' has been useful to economists as a way of referring to all of the activity that takes place within the network and the organizations that rely upon it for their existence (Braman 1996), so it might have been expected that the notion of network citizenship might arise. Early efforts to grapple with regulability in

the online environment went in this direction; Johnson and Post (1995) treated online communities as rule sets to which individuals can choose to commit, for example, and Lessig (1999), using other terminology, viewed participation in online environments as a matter of volunteer network political citizenship.

Certainly participants in specific online environments have been aggressively pursuing what they perceive as citizenship rights in particular virtual worlds (Lastowka and Hunter 2004; Taylor 2006). One study found that motivations for being active as a citizen in game worlds were much the same as they are geopolitically – active participation in civic life generates feelings of camaraderie and glory by association, as well as offering opportunities for public service and, ideally, self-determination (Michaly 2000). It might be argued that potential geopolitical threats so outweigh potential network political threats that the nature of citizenship in each domain cannot be considered equivalent. However, the realities of the integration of cyberspace with communications, energy, transportation and other fundamental societal infrastructure make this an unconvincing position.

Analysis of the Internet RFCs provides an opportunity to understand how the notion of citizenship evolved within the Internet design community, what it meant in practice, how citizenship practices affected design, and the diverse ways in which network citizenship interacts with geopolitical citizenship. This is of course not the first time that there have been interactions between preferences or habits of users of innovations in information and communication technologies and the requirements and protections of geopolitical citizenship. It is beyond the scope of this piece, but a comparative history of such interactions would be a valuable addition to the literature. The relationships become culturally visible when media moguls are commonly referred to as 'citizen' (Tunstall and Palmer 1991) and such individuals make a practice of changing citizenship in order to interact with different polities (Cunningham, Jacka and Sinclair 1998).

The concept of citizenship began to appear explicitly in the Internet RFCs in the years running up to commercialization of the network. Multiple types of relationships between the geopolitical and the network political are revealed in the treatment of citizenship within the RFCs. There are areas in which the two types of citizenship can come into conflict, and other times when they are complementary. Geopolitical and network political citizenship showed up within a year of each other, the first introduced by an American author, the second by an author from France. Among network political citizens, the distinction between those who are human and those that are not remains a latent problem likely to become more pressing in future.

GEOPOLITICAL CITIZENSHIP AND THE NETWORK

The notion that those who were online comprised a community of their own began to appear early on in ARPANet/Internet design process (Braman 2011) and continued to be further articulated as the number of people involved in that community grew significantly and internationally. The first reference to citizenship (rather than community) in the RFCs appeared in an argument for a national public network by the American founder of the Electronic Frontier Foundation (EFF), Mitch Kapor. Arguing that the government-funded National Research and Education Network (NREN) should be used as a test bed for such a network, Kapor turned to arguments put forward in support of the postal provision of the US Constitution to explain the need and provide

justification. The latter mandates the building of 'post roads' – a national road system – so that political representatives and their constituents can communicate via mail. This was considered a constitutional matter because two-way communications were essential to the democratic form being put into place. In this RFC, Kapor quoted US Senator John Calhoun's 1817 words about the value of such a universally accessible communication system, describing it as the 'nerves of the body politic' (RFC 1259, Kapor 1991: 21).[1]

The argument did not succeed when it came to the NREN, which became instead a model for a research-oriented network consortium involving a number of computationally intense research institutions connected via a network backbone with the highest bandwidth possible, always faster than that available to the general population on a commercial basis. In most, if not all, cases, this is accomplished with at least some government support. The availability of constitutional principles to support arguments for universal access to the Internet, however, remains. In a 1993 RFC titled, 'What Should We Plan Given the Dilemma of the Network?,' an author who had also drafted a proposed policy for NREN for the relatively short-lived US Office of Technology Assessment (OTA), an entity put into place to inform Congress, connected access to the Internet with the mainstream of political, social and economic life and pointed out that those without access would be second-class citizens in a self-reproducing cycle that would be difficult, if not impossible, to break (RFC 1527, Partridge 1991).

Rhonda Hauben and Michael Hauben published their book on 'netizens' in 1996, and by 1999 the renowned Vint Cerf (RFC 2555, RFC Editor 1999) and other RFC authors (see, e.g., RFC 2635, Hambridge and Lunde 1999) were using the term. In early usage, the word applied to those who live significant portions of their lives online and/or to those activities of people that take place when they are online, suggesting an orientation towards network political citizenship. Over time, however, the word has taken on a more activist connotation, suggesting that those referred to are active online in efforts to protect their civil liberties, whether those civil liberties themselves would be called into play for matters of geopolitical citizenship, whether offline (e.g., MacKinnon 2012) or online (e.g., Biegel 2001) or matters of network political citizenship.

Network designers understood that, as was mentioned in association with the first 'computer communications' conference in 1972, 'The social implications of this field are a matter of widespread interest that reaches society in almost all walks of life; education, medicine, research, business and government' (RFC 371, Kahn 1972: 1). Throughout the RFCs there are many references to government uses of the network, ranging from discussion of the general need to access criminal justice system information at a distance (RFC 144, Shoshani 1971) to very specific proposals, such as that for special information centres to help citizens respond to potential poisoning (RFC 5031, Schulzrinne 2008).

Designers expected the government to play particular roles vis-a-vis the network, such as running certification authorities in order to protect the security of citizen-government transactions (RFC 1984, IAB and IETF 1996). Many ways in which this is being done digitally for the provision of government services, in addition to Internet-based activities, were in widespread use by the close of the first decade of the twenty-first century (Lips 2013). Arguments for formal governmental namespaces by countries as different as New Zealand (RFC 4350, Hendrikx and Wallis 2006) and Latvia (RFC 4617, Kornijenko 2006) emphasized the range of functions a domain serves to ensure efficient

1. It was the UK Post Office that was the first postal service to show up in the RFCs as having reported an intention to put in a digital network, in the 'distant' future, in 1971 (RFC 164: Heafner 1971: 14).

government operations and services. It is worth noting that it was also the citizenship market that inspired the first spam, from a private firm selling help with the US immigration process (RFC 2235, Zakon 1997).

Citizens of the network began to appear as a type among categories of users of online services. In discussion of cross-registry ISP requirements, for example, 'general citizens of the Internet' are understood to be 'implementers of the software' along with 'large network operators, registry operators, and commercial entities offering value-added services' (RFC 3707, Newton 2004). In another document, citizens, as well as organizations and notaries, are suggested as users desiring long-term archive services; citizen interests were understood to include a range of evidentiary needs for purposes ranging from protection of intellectual and real property rights to documenting legal transactions and contracts, health and documentation of employment (RFC 4810, Wallace et al. 2007). It was understood that citizenship brings with it the need to authenticate citizenship identity; thus, the RFCs include discussion of naming schemes and electronic signatures (RFC 5126, Pinkas et al. 2008).

Country of citizenship is an attribute included in information collected for public key cryptography and LDAP (lightweight directory access protocol) accessible directories. The attribute is not a simple one. The text highlights the point that 'Determination of citizenship is a matter of law and is outside the scope of this document' (RFC 2985, Nystrom and Kaliski 2000: 10). The description of 'countryOfCitizenship' mentions that the information is as claimed, not as verified, and that there may be more than one country of citizenship. Country of residence is treated as a separate attribute which can also have several values. Both of these were part of the 'Natural Person' attribute set; identity change and multiplicity are acknowledged in this document. Acknowledging the possibility that an individual might have more than one citizenship, the RFC specifies that the identifier 'countryOfCitizenship' should, when it was present, contain at least one of the countries of citizenship claimed by the subject at the time that the certificate was issued, with more than one being allowed but not required. Where contested, as with 'countryOfResidence,' anonymity was to be allowed: 'Pseudonyms, nicknames and names with spelling other than defined by the registered name MAY be used' (RFC 2985, Nystrom and Kaliski 2000: 7).

The question of what kind of identification to require for certificates was a social as well as a technical problem because not all governments have, or had, official identification systems in place at the national level (RFC 2693, Ellison et al. 1999). Those issuing certificates are reminded to check the laws under which the certificate issuer operates, as well as those under which the entity issuing certificates operates, to see what might apply (RFC 3039, Santesson et al. 2001; RFC 3739, Santesson et al. 2004). When several different certificate authorities are involved, each certificate may be issued to a person as a citizen of a different country (RFC 5126, Pinkas et al. 2008). Names for certificate purposes can be changed in case of marriage and other legal name change processes (RFC 4043, Pinkas et al. 2005).

The word 'citizen' appeared once in the first version of the Internet security glossary (RFC 2828, Shirey 2000), and three times in the revised version (RFC 4949, Shirey 2007). The first reference, retained in the second version, was cultural, explaining that using the term 'handle' to refer to an online pseudonym derived from the traditions of citizens' band radio. The two uses of the word 'citizen' added to the second version involve privacy and security concerns and present the US government position. Citizens are an example of a group the individuals

of which could be provided with an 'anonymous credential' that warrants group membership but does not reveal the individual identity of the person bearing the credential (RFC 4949, Shirey 2007: 18). A 'highly protected environment' when it comes to classified information is an environment accessible only to US citizens with proper security clearances (RFC 4949, Shirey 2007: 62).

Normatively, the sense of community among those active online included an expectation that network political citizens have geopolitical responsibilities. Computer security incident response teams were to comprise ordinary citizens with ordinary powers, not necessarily members of law enforcement or security organizations (RFC 2350, Brownlee and Guttman 1998). The twentieth-anniversary celebration of ARPANet, in 1989, included a panel session on 'Impact on Government, Commerce and Citizenry' (RFC 1121, Postel et al. 1989: 5). Though explicit discussion of what 'good citizenship' might mean geopolitically is not found in these documents, there are implicit suggestions throughout of assumptions of classical ideas. Ideas about just what a good citizen is matter because they provide vocabularies, and therefore resources, for action (Thorson Huitema 2012). Features of good network citizenship did, however, come up in the RFCs and are discussed below.

NETWORK POLITICAL CITIZENSHIP

Not much more than a year after geopolitical citizenship surfaced in the RFCs, the notion of network political citizenship was also introduced. In December 1992, a French researcher proposing a routing protocol included, among the arguments offered in support of his approach the claim that particular elements of that protocol would make it easier for users to be 'good network citizens'. It is here that the foundational definition of the good network citizen still in play is first offered:

> A strong tradition of the Internet is the display of cooperative spirit: individual users are ready to suffer a bit and 'do the right thing' if this conduct can be demonstrated to improve the global state of the network – and also is not overly painful.
>
> (RFC 1383, Huitema 1992: 9)

As is so often the case, agreeing to do the right thing and knowing what the right thing to do in any given specific circumstances can be two very different things. Network designers, for example, easily reached a consensus that protocols that determined the sequence in which bits from messages from different message senders would be sent through the network should be 'fair.' Over just a few years' time, however, there was experimentation with four different approaches based on two fundamentally different ways of conceptualizing fairness, each serving particular types of communicators in different ways (Bares and Braman 2011). This problem links back to the long history of struggles over the extent to which governments should intervene to ensure universal access to the telecommunications network, and forward to the contemporary incarnation of that issue in network neutrality debates. The same problem, of course, appears in other communication regulation contexts. Among the reasons the 'Fairness Doctrine' was abandoned as a mandate to broadcasters to cover 'both' or 'all' sides of public issues was that it was impossible for the US Federal Communications Commission to come up with a viable approach to determining whether or not fairness had been achieved.

Another issue raised by the question of good network citizenship standards is the distinction between human and daemon, or machinic, citizens. For network designers, daemons are software and other electronic agents that are also network users (neither, in the Greek and medieval senses, human nor divine) and thus 'citizens' to be held to network citizenship standards and for which such standards need to be designed (Braman 2011). The expectation that the equipment comprising the network and the electronic processes involved will be good citizens appears at several points within the RFCs. A client machine should reissue a 'get notifications operation' within a defined time period in order to be a good network citizen (RFC 3996, Herriot et al. 2005: 12), and it was considered 'necessary to ensure that cellular hosts are good citizens of the Internet' (RFC 3316, Arkko et al. 2003: 3) while discussing specifications for IPv6. The same requirement was put forward for the iSCSI protocol (RFC 3347, Krueger and Haagens 2002), 'client' equipment such as printers (RFC 2996, Bernet 2000) and e-mail retransmission (RFC 5016, Thomas 2007). The fear is that pieces of equipment and software processes that are not good citizens will inappropriately, and potentially abusively, consume network and server resources.

The qualities of good network citizenship largely have to do with the extent to which an entity shares its own resources and respects those of others. Responsibilities begin, however, with compliance with the results of group decision-making and their formalization in the technical standards referred to as protocols. Network designers learned, by the early 1970s, that they could not assume compliance would be immediate, nor necessarily to be expected without additional effort. One RFC provides a list of things that must be done when initially joining the network in order to make sure that the new user is a good network citizen (RFC 2326, Schulzrinne et al. 1998).

Normative pressure was among the many techniques used to stimulate the compliance with protocols required in order for the network to run (Braman 2012). In RFC 1383 quoted from above, the importance of the network community was emphasized. Uniformity of queue size is recommended as an indicator of the extent to which a user is a good citizen: 'As the congestion is pushed to the sources, gateways which are bottlenecks can more easily detect someone not playing by the rules (sending datagrams in bursts) and deal with the offender' (RFC 1016, Prue and Postel 1987: 15). There are instances in which compliance and respect for the resources of others can be demonstrated in the same actions. In one example, it was argued that 'Major protocols will be assigned a unique value in byte 7 that will (among good citizens) not duplicate a value generated by a different protocol' (RFC 1044, Hardwick and Lekashman 1988: 7).

The Internet Advisory Board (IAB) presented a more systematic discussion of what is meant by good network citizenship in 'Ethics and the Internet' (RFC 1087, IAB 1989). The IAB opens by giving credit to the US National Science Foundation (NSF) for development of the position taken; these ethical issues were matters the NSF had to address in the course of funding a significant proportion of the development and expansion of the Internet. Five principles were endorsed by the IAB, defining as unethical and unacceptable any network behavior that:

(a) seeks to gain unauthorized access to the resources of the Internet,
(b) disrupts the intended use of the Internet,
(c) wastes resources (people, capacity, computer) through such actions,

(d) destroys the integrity of computer-based information and/or
(e) compromises the privacy of users (RFC 1087, IAB 1989: 2).

This RFC also includes justifications for network citizenship standards and asserts the IAB's jurisdictional rights in their regard. The Internet is described as 'an important national infrastructure' with society-wide critical functions analogous to those of other infrastructural systems such as roads, water, and power (RFC 1087, IAB 1989: 1). The fact that this infrastructure was designed and built at great cost, particularly to the US government – and therefore to its citizens – provided and provides a fiduciary rationale for ensuring that those resources were and are not wasted or abused.

Another corollary of the infrastructural status of the network is that it is of greatest value to everyone when it works. In its RFC on ethics, the IAB was in part responding to experience with the first deliberate network-wide attack, the event that spurred conceptualizing such events in biological terms. RFC 1135, about the worm that affected the Internet in 1988, is called 'Helmenthiasis' because it introduced a biological and epidemiological way of thinking about the effect of destructive software on the network (RFC 1135, Reynolds 1989). The IAB's position is that ultimate responsibility for the network's success in the face of such disruptions lies with its users, who should see it as a matter of professionalism (RFC 1087, IAB 1989).

In 2004, the IAB turned to the notion of network citizenship again in a discussion of the history of the end-to-end principle and its implementation in the Internet design process. In a document published during a period in which it was expected that tensions over standards would continue to increase, the IAB suggested that thinking in terms of the commonalities of network citizenship may help resolve what could otherwise be conflicts among diverse stakeholders that include ISPs, corporate network users, vendors of hardware and software, and governments. Where conflicts can be dissipated or prevented through technical design decisions, supporting 'good network citizen behavior' joins such matters as user choice and the integrity of end-to-end service as principles upon which decision-making should be based (RFC 3724, IAB 2004).

The resource sharing asked of good network citizens goes beyond the communal use of resources in a commons. In a commons, in its ideal form as theorized, use of resources by one citizen or group of citizens has no impact on the ability of others to use the same resources as well. In the Internet environment, being a good network citizen requires sharing resources even when doing so may come at some cost to oneself – even when someone else's use of resources can and does diminish your own ability to use the same resources or deprive you of it altogether. One example of this was provided by promoters of a domain-name based routing system (DNS) that would shift the managerial focus from pathways to end points. Authors of this RFC claimed that users would be willing to make the change 'Because they are good network citizen (*sic*) and want to suffer their share in order to ease the general burden of the Internet' (RFC 1383, Huitema 1992: 9). It is worth noting that this expectation of altruism was offered in tandem with the expectation that users would also be interested to accept the proposal being offered because they would have financial motivations for doing so. As the exhaustion horizon of the IPv4 address space became visible, there was even a request to hosts with large numbers of unused IP addresses to return them to the Internet Assigned Numbers Authority (IANA) for redistribution to those who were in need and

could not otherwise get them (RFC 1971, Thomson and Narten 1996). This sense that one gives of oneself for the greater good of the whole is very much a characteristic of the nationalism expressed by devoted geopolitical citizens.

Documents urging network users to respect the resources of others sometimes yield a sense of a loss of shared culture, including online behavioral norms, with the expansion of the size of the network community. This change was directly addressed in an RFC wonderfully titled, 'DON'T SPEW,' that offered guidelines for handling spam. Critiquing those who see the network as a windfall of potential customers and thus hold that 'all people should at least hear about the one true religion or political party or process' (RFC 2635, Hambridge and Lunde 1999: 2), the authors describe norm development. Good network citizens, they contend, view unsolicited e-mail as 'theft of service,' since the recipient must pay for it. This was the same argument used in the United States to make it illegal to send the equivalent of junk mail to fax machines.

It is around the standards for good network citizenship that the distinction between experienced network users and those new to the Internet received emphasis in a 2001 document about how to advertise online responsibly. The question was of such importance because of differences in types of uses. Prior to commercialization most activity involved research and experimentation with the network itself. A high proportion of users joining the network after 1993, when it was made available to all users for all purposes, were involved in commercial, entertainment, and other types of uses. In this context, Gavin and his colleagues argued in a 2001 RFC update of rules for advertising online responsibly that,

> There are stereotypes that must be broken before continuing. Not all persons who are new to the Internet are ignorant of the 'Net's history and evolution, or its proper and ethical uses. Nor are all experienced, long-term Netizens against the use of the Internet for advertising, marketing, or other business purposes. Where these two groups can find commonality is in their opposition to the use of the Internet in irresponsible ways.
>
> (RFC 3098, Gavin et al. 2001: 2)

Free speech, from this perspective, is based in respect for the resources and activities of others and in putting restraints on one's own activities in order to benefit the network as a whole. Thus, for example, the authors of RFC 2518 (Goland et al. 1999) and its successor RFC 4918 (Dusseault 2007) argued that incorporating overwrite protection into distributed authoring functions was necessary if the clients involved were to be good network citizens.

INTERACTIONS BETWEEN THE GEOPOLITICAL AND THE NETWORK POLITICAL

There are a number of ways in which the two citizenship orientations – around the state and around the network – interact. In many areas the two complement each other, but in some they come into tension.

At the most abstract level, there is uncertainty regarding how to draw a line between the geopolitical and the network political. The Internet Advisory Board (IAB) took the position, in 2004, that resolving conflicts among Internet service providers (ISPs), businesses, governments and users is not the

responsibility of the Internet Engineering Task Force (IETF), the entity that manages the design process, even if those issues could be resolved technically (RFC 3724; Kempf and Austin 2004). Those writing the code for the Internet, that is, took the position within the RFCs that code is *not* law. This was based on the argument that the IETF could act on the responsibilities that would attend accepting code in the sense of Internet design and architecture decisions as law, but should not do so because it is not within its jurisdiction to deal with social and legal matters. The RFCs also provide at least one example of the reverse – 'law is code' – or use of the law as a model for how to write code. The author of a 2004 document drew on US court cases for his recommendation that trespass law be applied to spam and his encouragement that a technical equivalent for no trespassing signs – the 'no soliciting SMTP service extensions' – be developed as responses to the 'spam pandemic' then underway (RFC 3865, Malamud 2004: 1).

It was the realization, around 1970–1971, that network designers had to take international telecommunications tariffs and other regulatory matters into account when the Internet linked with networks in other countries (Braman 2012), that was the first discussion of tensions between network political and geopolitical citizenship in RFCs. Jurisdictional issues were also problematic, leading Internet designers to urge prioritization of the network political over the geopolitical. As they struggled with legal differences in treatment of electronically transmitted information flows – what was called 'transborder data flow' (TDF, or TBDF) at the time – there was a call for national governments to change their laws so that they would all be alike in this area (legal harmonization) to solve the technical problem (RFC 828, Owen 1982). It is in the area of security, however, that differences in needs, and therefore differences in how responsibilities are defined, are vividly evident.

As discussed in a section on 'Good Internet Citizenship,' in an RFC that presented itself as a *Site Security Handbook*, determining the right thing to do when there is a security incident is problematic because the two different types of citizenship require two different responses. The handbook described the problem in the course of a discussion of how site and network needs, on one hand, and investigative agency needs, on the other, may diverge. When there is an attack, 'Your site may want to get back to normal business by closing an attack route, but the investigative agency may want you to keep this route open' (RFC 1244, Holbrook and Reynolds 1991: 76). Harms for a site that remains open under attack will be reputational in addition to other losses. Thus, when an attack occurs, a site must consider a complex set of trade-offs that include not only immediate site interests but also resources available, jurisdictional boundaries, possible damage to others and whether or not failure to cooperate with an agency may redound badly for the site if it turns to the agency for help for itself, subsequently.

Needs of the government and those of the network, then, must be balanced. The advice of the *Site Security Handbook* is based on the policy principles for network citizens put forward by the IAB in 1989 discussed above (RFC 1087, IAB 1989). Applying those principles to the situation in which network political and geopolitical interests collide, the authors conclude the following:

> Providing that there is no damage to your system and others, the most responsible course of action is to cooperate with the participating agency by leaving your compromised system on. This will allow monitoring

> (and, ultimately, the possibility of terminating the source of the threat to systems just like yours). On the other hand, if there is damage to computers illegally accessed through your system, the choice is more complicated: shutting down the intruder may prevent further damage to systems, but might make it impossible to track down the intruder. If there has been damage, the decision about whether it is important to leave systems up to catch the intruder should involve all of the organizations [a]ffected.
>
> (RFC 1244, Holbrook and Reynolds 1991: 76)

Acknowledging the political nature of the many interdependencies involved, the IETF ends this paragraph by noting that those who do not cooperate with law enforcement and criminal justice agencies may be concerned about the extent to which they could themselves expect protection from the same agencies in the future.

This type of tension between the geopolitical and the network political receives attention again in the revised *Site Security Handbook*, published in RFC 2196 in 1997, after a number of years of experience with a commercialized Internet. By this time individual site owners had become much more sensitive to liability concerns should the network or their sites become compromised. The two choices available in such a situation were described as either watching the intruder to determine its identity or cleaning up the damage and shutting the intruder out of the system. It was noted that there may be legal liabilities should a site choose to remain open if damage is subsequently caused to other sites. A proactive stance regarding responsibilities to others was recommended more than six years earlier: 'Being a good Internet citizen means that you should try to alert other sites that may have been impacted by the intruder. These affected sites may be readily apparent after a thorough review of your log files' (RFC 2196, Fraser 1997: 59).

The temptation to pursue an invader is also confronted in the revised *Site Security Handbook*, which warns:

> It is one thing to protect one's own network, but quite another to assume that one should protect other networks. During the handling of an incident, certain system vulnerabilities of one's own systems and the systems of others become apparent. It is quite easy and may even be tempting to pursue the intruders in order to track them. Keep in mind that at a certain point it is possible to 'cross the line,' and, with the best of intentions, become no better than the intruder.
>
> (RFC 2196, Fraser 1997: 59)

The handbook recommends a conservative and prudent stance in such situations, declining to become involved with any computer in a manner that isn't intended to be public and proactively locating and communicating with a human at the site about which there is concern.

CONCLUSIONS

Conceptualizations of citizenship matter, of course, because they provide the affordances for agency. We are growing accustomed to thinking of many of our subjects of study as socio-technical in nature, and beginning to develop what might be referred to as socio-technical research methods, an adaptation of

techniques to take into account relationships between humans and machines of diverse kinds. We are only beginning to think through law and policy from a socio-technical perspective, and both of those are bound up with socio-technical approaches to the very basics of the political system.

During the same years that the problem of designing what we now call the Internet was being addressed, there were discussions within several social science literatures about alternative ways of formulating the concept of citizenship and/or of operationalizing it or its expectations, including literatures on both global citizenship and on citizenship as defined in relationship to technology. The research reported upon here asked the question of how those involved in the technical design process for what we now call the Internet thought about citizenship-related matters in the course of their technology design and network architecture work. The research was conducted through analysis of the technical document series that served as both the medium for consensus building and as the historical record of those processes, the Internet Requests for Comments, or RFCs, 1969–2009.

What the research found should be useful to all of those working on the socio-technical boundary from whatever discipline. To those responsible for ensuring a network that offers all the capacities the Internet offers when unconstrained, the first pass at building a network (while simultaneously conceptualizing and reconceptualizing just what that network should be) very quickly yielded a keen sense of the importance of both daemon and human citizens; further research, conceptualization and theorization in this area would be helpful for those currently building out the domain of robot law and in other areas of the law in which machinic liability is a matter of concern. The research found that the concept of network citizenship had very real implications both for technical standard setting and for behavioral norms of human users, pushing forward the literature on the diverse types of relationships between technology and citizenship into a domain in which it will be easier to link that conversation up with matters of the law. And it found that commitments to the infrastructure through which almost all of our social processes unfold today could run directly counter to those of the geopolitical governments to which network users also have responsibilities and allegiances – a finding that should press those concerned about the nature of governance in the digital environment to probe for theoretical and conceptual frames that would provide a foundation for citizenship in a genuinely socio-technical world.

ACKNOWLEDGEMENT

This material is based on work supported by the National Science Foundation under Grant No. 0823265 and by the University of Wisconsin-Milwaukee Office of Undergraduate Research. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author. Thanks to Alyse Below Rodich for her work as project manager.

REFERENCES

Abbate, J. (1999), *Inventing the Internet*, Cambridge, MA: MIT Press.

Barbero, I. (2012), 'Expanding acts of citizenship: The struggles of *Sinpapeles* migrants', *Social & Legal Studies*, 21: 4, pp. 529–47.

Bares, N. J. and Braman, S. (2011, May), 'Fair queuing: The ethics of network gateways', Presented to GIGANet, Washington, DC.

Biegel, S. (2001), *Beyond Our Control? Confronting the Limits of Our Legal System in the Age of Cyberspace*, Cambridge, MA: MIT Press.

Bovens, M. B. (2002), 'Information rights: Citizenship in the information society', *The Journal of Political Philosophy*, 10: 3, pp. 317–41.

Braithwaite, J. and Drahos, P. (2000), *Global Business Regulation*, Cambridge: Cambridge University Press.

Braman, S. (1996), 'Interpenetrated globalization: Scaling, power, and the public sphere', in S. Braman and A. Sreberny-Mohammadi (eds), *Globalization, Communication, and Transnational Civil Society*, Greenskill, NJ: Hampton Press.

—— (2007a), *Change of State: Information, Policy, and Power*, Cambridge, MA: MIT Press.

—— (2007b), 'The ideal vs. the real in media localism: Regulatory implications', *Communication, Law, and Policy*, 12: 3, pp. 231–78.

—— (2011), 'The framing years: Policy fundamentals in the Internet design process, 1969–1979', *The Information Society*, 27: 5, pp. 295–310.

—— (2012), 'Internationalization of the Internet by design: The first decade', *Global Media and Communication*, 8: 1, pp. 27–45.

Caporaso, J. A. (2000), 'Transnational markets, thin citizenship, and democratic rights in the European Union: From cradle to grave or from job to job?', Presented to the International Studies Association, Los Angeles, CA, March.

Charnovitz, S. (2003), 'The emergence of democratic participation in global governance (Paris, 1919)', *Indiana Journal of Global Legal Studies*, 10: 1, pp. 45–77.

Cunningham, S., Jacka, E. and Sinclair, J. (1998), 'Global and regional dynamics of international television flows', in D. Thussu (ed.), *Electronic Empires: Global Media and Local Resistance*, London: Arnold, pp. 177–92.

Dandeker, C. (1990), *Surveillance, Power and Modernity: Bureaucracy and Discipline from 1700 to the Present Day*, New York: St. Martin's Press.

Davis, G. F., Kahn, R. L. and Zaid, M. N. (1990), 'Contracts, treaties, and joint ventures', in R. L. Kahn and M. N. Zaid (eds), *Organizations and Nation-States: New Perspectives on Conflict and Cooperation*, San Francisco: Jossey-Bass Publishers, pp. 19–54.

Eizaguirre, S., Pradel, M., Terrones, A., et al. (2012), 'Multilevel governance and social cohesion: Bringing back conflict in citizenship practices', *Urban Studies*, 49: 9, pp. 1999–2016.

Elam, M. and Bertilsson, M. (2003), 'Consuming, engaging and confronting science', *European Journal of Social Theory*, 6: 2, pp. 233–51.

Elkins, D. J. (1997), 'Globalization, telecommunication, and virtual ethnic communities', *International Political Science Review*, 18: 2, pp. 139–52.

Erjavec, K. (2009), 'The "Bosnian war on terrorism"', *Journal of Language and Politics*, 8: 1, pp. 5–27.

Featherstone, M. (ed.) (1990), 'Global culture: An introduction', in *Global Culture: Nationalism, Globalization and Modernity*, London: Sage Publications, pp. 1–14.

Felt, U. and Fochler, M. (2010), 'Machineries for making publics: Inscribing and de-scribing publics in public engagement', *Minerva*, 48: 3, pp. 219–38.

Flear, M. L. and Pickersgill, M. D. (2013), 'Regulatory or regulating publics? The European Union's regulation of emerging health technologies and citizen publication', *Medical Law Review*, 21: 1, pp. 39–70.

Frankenfeld, P. J. (1992), 'Technological citizenship: A normative framework for risk', *Science, Technology, & Human Values*, 17: 4, pp. 459–84.

Held, D. (1989), *Political Theory and the Modern State: Essays on State, Power, and Democracy*, Stanford: Stanford University Press.
Henderson, A., Jeffery, C., Wincott, D., et al. (2013), 'Reflections on the "devolution paradox": A comparative examination of multilevel citizenship', *Regional Studies*, 47: 3, pp. 303–22.
Hermes, J. (2006), 'Hidden debates: Rethinking the relationship between popular culture and the public sphere', *Javnost/The Public*, 13: 4, pp. 27–44.
Johnson, D. R. and Post, D. (1995), 'Law and borders: The rise of law in cyberspace', *Stanford Law Review*, 48: 1995, pp. 1367–462.
Kaarsholm, P. (2013), 'Diaspora or transnational citizens? Indian Ocean networks and changing multiculturalisms in South Africa', *Social Dynamics*, 38: 3, pp. 454–66.
Lastowka, F. G. and Hunter, D. (2004), 'The laws of the virtual worlds', *California Law Review, 2004*, pp. 1–73.
Koenig-Archibugi, M. (2012), 'Fuzzy citizenship in global society', *Journal of Political Philosophy*, 20: 4, pp. 456–480.
Leca, J. (1992), 'Questions on citizenship', in C. Mouffe (ed.), *Dimensions of Radical Democracy: Pluralism, Citizenship, Community*, London and New York: Verso, pp. 17–32.
Lee, M. (2009), 'Constructed global space, constructed citizenship', *Javnost–The Public*, 16: 3, pp. 21–37.
Lessig, L. (1999), *Code and Other Laws of Cyberspace*, New York: Basic Books.
Lips, M. (2013), 'Reconstructing, attributing and fixating citizen identities in digital-era government', *Media, Culture & Society*, 35: 1, pp. 61–70.
MacKinnon, R. (2012), 'The netizen', *Development*, 55: 2, pp. 201–04.
Marsden, C. T. (2011), *Internet Co-Regulation: European Law, Regulatory Governance and Legitimacy in Cyberspace*, Cambridge: Cambridge University Press.
Marsh, D. (1998), *Comparing Policy Networks*, Cambridge: Open University Press.
Marshall, T. H. (1950), *Citizenship and Social Class and Other Essays*, Cambridge: Cambridge University Press.
Mattelart, A. (1987), 'Informatics and micro-revolutions in the Third World', in J. D. Slack and F. Fejes (eds), *The Ideology of the Information Age*, Norwood, NJ: Ablex, pp. 243–63.
Michaly, M. (2000, March 19), 'Constructive politics in a massively multiplayer online roleplaying game', *Gamasutra*, http://www.gamasutra.com/blogs/ Accessed 13 June 2004.
Mouffe, C. (ed.) (1992), 'Democratic citizenship and the political community', in *Dimensions of Radical Democracy: Pluralism, Citizenship, Community*, London and New York: Verso, pp. 225–39.
Mueller, M. (2002), *Ruling the Root: Internet Governance and the Taming of Cyberspace*, Cambridge, MA: MIT Press.
Nussbaum, M. C. (2003, Winter), 'Cultivating humanity in legal education', *University of Chicago Law Review*, 70, pp. 265–79.
Pathak, P. (2013), 'From new labour to new conservatism: The changing dynamics of citizenship as self-government', *Citizenship Studies*, 17: 1, pp. 61–75.
Randeira, S. (2007), 'The state of globalization: Legal plurality, overlapping sovereignties and ambiguous alliances between civil society and the cunning state in India', *Theory, Culture & Society*, 24: 1, pp. 1–33.
Schudson, M. (1998), *The Good Citizen: A History of American Civic Life*, New York: Martin Kessler Books.

Stevenson, N. (2006), 'Technological citizenship: Perspectives in the recent work of Manuel Castells and Paul Virilio', *Sociological Research Online*, 10: 3.
Strijbos, S. (2001), 'Global citizenship and the real world of technology', *Technology in Society*, 23: 4, pp. 525–33.
Taylor, T. L. (2006, September), 'Beyond management: Considering participatory design and governance in player culture', *First Monday*, Special issue number 7, http://firstmonday.org/issues/issue11_9/taylor/index.html.
Thorson, K. (2012), 'What does it mean to be a good citizen? Citizenship vocabularies as resources for action', *Annals of the American Academy of Political and Social Science*, 644: 1, pp. 70–85.
Tunstall, J., and Palmer, M. (1991), *Media Moguls*, New York: Routledge.
Turner, F. (2006), *From Counterculture to Cyberculture: Stewart Brand, the Whole Earth Network, and the Rise of Digital Utopianism*, Chicago: University of Chicago Press.
Turner, B. (1992), 'Outline of a theory of citizenship', in C. Mouffe (ed.), *Dimensions of Radical Democracy: Pluralism, Citizenship, Community*, London and New York: Verso, pp. 33–62.
Yeatman, A. (1994), *Postmodern Revisionings of the Political*, New York: Routledge.
Valkenburg, G. (2012), 'Sustainable technological citizenship', *European Journal of Social Theory*, 15: 4, pp. 471–87.

RFCS CITED

RFC 144, 'Data sharing on computer networks', A. Shoshani, April 1971.
RFC 164, 'Minutes of network working group meeting, 5/16 through 5/19/71', J. F. Heafner, May 1971.
RFC 371, 'Demonstration at international computer communications conference', R. E. Kahn, July 1972.
RFC 828, 'Data communications: IFIP's international "network" of experts', K. Owen, August 1982.
RFC 1016, 'Something a host could do with source quench: The Source Quench Introduced Delay (SQuID)', W. Prue and J. Postel, July 1987.
RFC 1044, 'Internet protocol on network system's HYPERchannel: Protocol specification', K. Hardwick and J. Lekashman, February 1988.
RFC 1087, 'Ethics and the internet', Defense Advanced Research Projects Agency, Internet Activities Board, January 1989.
RFC 1121, 'Act one – The poems', J. Postel, L. Kleinrock, V. G. Cerf, and B. Boehm, September 1989.
RFC 1135, 'The helmenthiasis of the internet, J. Reynolds, December 1989.
RFC 1244, 'Site security handbook', J. P. Holbrook and J. K. Reynolds, July 1991.
RFC 1259, 'Building the open road: The NREN as test-bed for the national public network', M. Kapor, September 1991.
RFC 1383, 'An experiment in DNS based IP routing', C. Huitema, December 1992.
RFC 1527, 'Isochronous applications do not require jitter-controlled networks', C. Partridge, September 1991.
RFC 1971, 'IPv6 stateless address autoconfiguration', S. Thomson and T. Narten, August 1996.
RFC 1984, 'IAB and IESG statement on cryptographic technology and the internet, IAB and IESG', August 1996.

RFC 2196, 'Site security handbook', B. Fraser, September 1997.
RFC 2235, 'Hobbes' internet timeline', R. Zakon, November 1997.
RFC 2326, 'Real Time Streaming Protocol (RTSP)', H. Schulzrinne, A. Rao, and R. Lanphier, April 1998.
RFC 2350, 'Expectations for computer security incident response', N. Brownlee and E. Guttman, June 1998.
RFC 2518, 'HTTP extensions for distributed authoring – WEBDAV', Y. Goland, E. Whitehead, A. Faizi, S. Carter, and D. Jensen', February 1999.
RFC 2555, '30 Years of RFCs', RFC Editor, et al. April 1999.
RFC 2635, 'DON'T SPEW: A set of guidelines for mass unsolicited mailings and postings (spam*)', S. Hambridge and A. Lunde, June 1999.
RFC 2693, 'SPKI certificate theory', C. Ellison, B. Frantz, B. Lampson, R. Rivest, B. Thomas, and T. Ylonen, September 1999.
RFC 2828, 'Internet security glossary', R. Shirey, May 2000.
RFC 2985, 'PKCS #9: Selected object classes and attribute types version 2.0.', M. Nystrom and B. Kaliski, November 2000.
RFC 2996, 'Format of the RSVP DCLASS object', Y. Bernet, November 2000.
RFC 3039, 'Internet X.509 public key infrastructure qualified certificates profile', S. Santesson, W. Polk, P. Barzin, and M. Nystrom, January 2001.
RFC 3098, 'How to advertise responsibly using e-mail and newsgroups or – How NOT to $$$$$ MAKE ENEMIES FAST! $$$$$', T. Gavin, D. Eastlake 3rd, and S. Hambridge, April 2001.
RFC 3316, 'Internet Protocol Version 6 (IPv6) for some second and third generation cellular hosts', J. Arkko, G. Kuijpers, H. Soliman, J. Loughney, and J. Wiljakka, April 2003.
RFC 3347, 'Small Computer Systems Interface protocol over the Internet (iSCSI) requirements and design considerations', M. Krueger and R. Haagens, July 2002.
RFC 3707, 'Cross Registry Internet Service Protocol (CRISP) requirements', A. Newton, February 2004.
RFC 3724, 'The rise of the middle and the future of end-to-end: Reflections on the evolution of the internet architecture', J. Kempf and R. Austin (eds), IAB, March 2004.
RFC 3739, 'Internet X.509 Public key infrastructure: Qualified certificates profile', S. Santesson, M. Nystrom, and T. Polk, March 2004.
RFC 3865, 'A no soliciting Simple Mail Transfer Protocol (SMTP) service extension', C. Malamud, September 2004.
RFC 3996, 'Internet Printing Protocol (IPP): The "ippget" delivery method for event notifications', R. Herriot, T. Hastings, and H. Lewis, March 2005.
RFC 4043, 'Internet X.509 public key infrastructure permanent identifier', D. Pinkas and T. Gindin, May 2005.
RFC 4350, 'A Uniform Resource Name (URN) formal namespace for the New Zealand Government', F. Hendrikx and C. Wallis, February 2006.
RFC 4617, 'A Uniform Resource Name (URN) formal namespace for the Latvian national government integration project', J. Kornijenko, August 2006.
RFC 4810, 'Long-term archive service requirements', C. Wallace, U. Pordesch, and R. Brandner, March 2007.
RFC 4918, 'HTTP extensions for web distributed authoring and versioning (WebDAV)', L. Dusseault (ed.), June 2007.
RFC 4949, 'Internet security glossary, Version 2', R. Shirey, August 2007.
RFC 5016, 'Requirements for a DomainKeys Identified Mail (DKIM) signing practices protocol', M. Thomas, October 2007.

RFC 5031, 'A Uniform Resource Name (URN) for emergency and other well-known services', H. Schulzrinne, January 2008.
RFC 5126, 'CMS Advanced Electronic Signatures (CAdES)', D. Pinkas, N. Pope, and J. Ross, March 2008.

SUGGESTED CITATION

Braman, S. (2013), 'The geopolitical vs. the network political: Internet designers and governance', *International Journal of Media and Cultural Politics* 9: 3, pp. 277–296, doi: 10.1386/macp.9.3.277_1

CONTRIBUTOR DETAILS

Sandra Braman's work on the co-construction of law, technology and society has been supported by the Rockefeller Foundation, Ford Foundation and the Open Society Institute as well as the National Science Foundation. Her books include *Change of State: Information, Policy, and Power* (MIT Press), first published in 2006 and currently undergoing revision for a second edition, as well as the edited volumes *The Emergent Global Information Policy Regime, Biotechnology and Communication: The Meta-Technologies of Information* and *Communication Researchers and Policy-Making*. She is current Chair of the Law Section of the International Association of Media and Communication Research and former Chair of the Communication Law and Policy Division of the International Communication Association. She is currently serving as Professor of Global Studies and Professor of Communication at the University of Wisconsin-Milwaukee.

Contact: Global Studies, PO Box 413, Milwaukee, WI 53201, USA.
E-mail: braman@uwm.edu